Claims

1. A computer-implemented method for detection of items stored in a computer system such as computer code, data or information characterised in that it comprises obtaining (18) a signature by reading code comprising at least part of a program capable of introducing the items, the code incorporating sufficient data to characterise the program adequately, using the code as the signature, comparing (90) the signature with files stored on the computer system, and, if a match with the signature is found, providing an indication thereof (96).

2. A method according to Claim 1 characterised in that the indication incorporates an identification of at least one of
   a) an item responsible for the match,
   b) the nature of the item,
   c) the item's location in the computer system, and
   d) the matching signature.

3. A method according to Claim 1 characterised in that the items are steganographic items.

4. A method according to Claim 1 characterised in that the code that is read is one of the following:
   a) a continuous sequence of program code;
   b) a continuous sequence of program code and beginning where its program begins,
   c) a continuous sequence of program code but not more than 5% and not less than 0.167% of its program's code;
   d) a program kernel;
   e) a .DDL or .ocx file; and
   f) code implementing both write to and read from a file.

5. A method according to Claim 1 characterised in that asserted file type is ignored when comparing (90) files with the signature.

6. A method according to Claim 1 characterised in that the step (90) of comparing the signature with files is for each file preceded by checking the respective real file type by reading the start of the file and excluding files having prearranged initial byte sequences from comparing with the signature.

7. A method according to Claim 1 characterised in that files not accessible by a system administrator are excluded from comparison with the signature.

8. A method according to Claim 1 characterised in that files compared with the signature include logical wastebasket files deleted files and compressed files.

9. A method according to Claim 1 characterised in that files compared with the signature include self-extracting executable files and polymorphic files.

10. A method according to Claim 1 characterised in that in respect of some prearranged files no indication as aforesaid is given despite their containing code which matches a signature.

11. Computer apparatus for detection of stored items such as computer code, data or information characterised in that the apparatus is programmed to:

a) obtain (18) a signature by reading code comprising at least part of a program capable of introducing the items, the code incorporating sufficient data to characterise the program adequately,

b) use the code as the signature,

c) compare (90) the signature with files stored on the computer apparatus, and

d) if a match with the signature is found, providing an indication thereof (96).

12. Apparatus according to Claim 11 characterised in that the indication incorporates an identification of at least one of:

a) an item responsible for the match,

b) the nature of the item,

c) the item's location in the computer system, and

d) the matching signature.

13. Apparatus according to Claim 11 characterised in that the items are steganographic items.

14. Apparatus according to Claim 11 characterised in that the code of the signature is one of the following:

a) a continuous sequence of program code;

b) a continuous sequence of program code and beginning where its program begins,

c) a continuous sequence of program code but not more than 5% and not less than 0.167% of its program's code;

d) a program kernel;

e) a .DDL or .ocx file; and

f) code implementing both write to and read from a file.

15. Apparatus according to Claim 11 characterised in that it is programmed to ignore asserted file type when comparing files with the signature.

16. Apparatus according to Claim 11 characterised in that before comparing (90) the signature with files it is programmed to check for each file the respective real file type by reading the start of the file and excluding files having prearranged initial byte sequences.

17. Apparatus according to Claim 11 characterised in that it is programmed to exclude files not accessible by a system administrator from comparison with the signature.

18. Apparatus according to Claim 11 characterised in that it is programmed to compare (90) with the signature logical wastebasket files, deleted files and compressed files.

19. Apparatus according to Claim 11 characterised in that it is programmed to compare (90) with the signature self-extracting executable files and polymorphic files.

20. Apparatus according to Claim 11 characterised in that it is programmed (72, 74) to give no indication as aforesaid in respect of some prearranged files despite their containing code which matches a signature.

21. Computer software for use in detection of items stored in a computer system such as computer code, data or information characterised in that the software contains instructions for controlling computer apparatus to obtain (18) a signature by reading code comprising at least part of a program capable of introducing the items, the code incorporating sufficient data to characterise the program adequately, to use the code as the signature, to compare (90) the signature with files stored on the computer apparatus, and, if a match with the signature is found, to provide an indication thereof (96).

22. Computer software according to Claim 21 characterised in that the indication incorporates an identification of at least one of

a) an item responsible for the match,

b) the nature of the item,

c) the item's location in the computer system, and

d) the matching signature.

23. Computer software according to Claim 21 characterised in that the items are steganographic items.

24. Computer software according to Claim 21 characterised in that the signature is one of the following:

a) a continuous sequence of program code;

b) a continuous sequence of program code and beginning where its program begins,

c) a continuous sequence of program code but not more than 5% and not less than 0.167% of its program's code;

d) a program kernel ;

e) a .DDL or .ocx file; and

f) code implementing both write to and read from a file.

25. Computer software according to Claim 21 characterised in that it contains instructions for controlling computer apparatus to ignore asserted file type when comparing files with the signature.

26. Computer software according to Claim 21 characterised in that it contains instructions for controlling computer apparatus to check real file type by reading the start of the file and exclude files having prearranged initial byte sequences from comparison with the signature, and to do so prior to comparing the signature with files.

27. Computer software according to Claim 21 characterised in that it contains instructions for controlling computer apparatus exclude from comparison with the signature files not accessible by a system administrator.

28. Computer software according to Claim 21 characterised in that it contains instructions for controlling computer apparatus to compare (90) with the signature logical wastebasket files, deleted files and compressed files.

29. Computer software according to Claim 21 characterised in that it contains instructions for controlling computer apparatus to compare (90) with the signature self-extracting executable files and polymorphic files.

30. Computer software according to Claim 21 characterised in that its instructions provide for computer apparatus controlled by it to give no indication as aforesaid in respect of some prearranged files despite their containing code which matches a signature.